

Autor:
Arkadiusz Ziobiewicz
kl. VIIb

Gimnazjum z
Oddziałem Integracyjnym im.
Jana Pawła II
w Kaluży

Ochrona danych osobowych

w pigułce

#1 Prawo

Według ustawy z dnia 29 sierpnia 1997 r. o wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoba możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, biologiczne, umysłowe, ekonomiczne, kulturalne lub społeczne).

Czym są dane osobowe?

Do danych osobowych zaliczamy np.: imię, nazwisko, adres osoby.

NIP, PESEL, linie papilarne, DNA, waga, siatkiówki, informacje o sytuacji finansowej osoby i adres mailowy zawierający konkretne imię bądź nazwisko; adres IP komputera danej osoby.

Dane osobowe, zarówno zwykłe (#1) jak i wrażliwe (#2) należy jednakowo chronić.

#2 Dane wrażliwe

Ważnym elementem tożsamości są także tzw. dane wrażliwe. Obejmują one elementy, których nie zawierają dokumenty prawne; jednakże są one cechą pozwalającą na identyfikację konkretnego obywatela.

Przykładowe dane wrażliwe to: pochodzenie etniczne, poglądy polityczne i religijne, przynależność do partii/organizacji, orientacja seksualna, stan zdrowia czy informacje o karalności.

Jak chronić dane osobowe?

czyli o ochronie prywatności i bezpieczeństwie informacji osobowych

#3 Informacje o sobie

Prywatne informacje o np. naszym miejscu zamieszkania, adresie e-mail czy numerze telefonu należy podawać tylko bliskim nam osobom. Pod żadnym pozorem nie można przekazać tych danych nowo poznanemu znajomemu - nigdy nie wiadomo, jakie może mieć intencje wobec nas.

#5 Wykorzystanie danych osobowych

Biorąc udział w różnych konkursach czy przedsięwzięciach często otrzymujemy zaproszenia do przetwarzania danych osobowych. Nie traktujmy tego jako zwykłej notki prawnej czy kolejnego wymysłu władzy państwa na celu uprzykrzyć życie i co najmniej nie podpisujemy od razu. Najpierw należy zastanowić się, czy umieszczenie naszego wizerunku oraz imienia i nazwiska np. na stronie www nie spowoduje żadnych negatywnych konsekwencji.

#4 Numer konta, hasła itp.

Są one rzeczy prywatne i tylko ich posiadacz ma prawo zasiedzieć. Jeżeli udostępnimy hasło do WI-FI, przewidujemy, że nie będziemy napisać o nim podany komuś numer konta i PIN, istnieje bardzo duże zagrożenie, że pieniądze znajdujące się tam mogą zostać wypłacone bez naszej wiedzy.

#6 Bezpieczeństwo danych w Internecie

Sieć Internet to miejsce, w którym nasze dane osobowe mogą najłatwiej zostać wykradzione. Wystarczy brak dokładnych zabezpieczeń profilu na określonym portalu, a także kilka publicznie udostępnionych zdjęć, by być potencjalnie narażonym na niebezpieczeństwo z prawem wykorzystanie naszych danych osobowych. Zawsze trzeba pamiętać o tym, że ktoś po kradzieży danych czy zdjęć może zacząć nas szantażować, poniżać, a także tworzyć np. kompromitujące fotomontaże czy rozsyłać fotografie kolejnym internautom. By tego uniknąć, należy stosować się do kilku ważnych zasad.

1. Nigdy nie wolno przysłać swoich zdjęć nowo poznanym osobom, do której nie ma się zaufania. Należy uważać, kto przysłał je kolejnym „przyjaciółkom”. Należy nie odczytywać wiadomości, w których widnieją wizerunki osób trzecich (zrzut ekranu, fotomontaż).

2. Aby utrzymać nie wykorzystaniem naszych danych osobowych przez osoby trzecie powinniśmy od razu po założeniu konta wyczyścić wszystkie najwięcej ustawień prywatności takich jak np. brak możliwości przeglądania naszych zdjęć przez osoby niebędące naszymi znajomymi czy niewidoczność naszego konta dla niezalogowanych.

3. Należy również pamiętać o tym, by na różnych czasach zakładać konta, w których nie ma naszej informacji o naszym imieniu/nazwisku. Zawsze łatwiej jest znaleźć kontem np. Janka Kowalskiego niż np. karpak31234.

4. Warto zabezpieczyć dostęp do naszego komputera i kont przez silne hasło (nie takie, które zawiera duże i małe znaki, liczby, a najlepiej jeżeli jest tylko kombinacją znaków, a nie konkretnym słowem. Silne hasło to np. W621Kz69D0).

NIGDY NIE MOŻNA PODAĆ NIKOMU HASŁA. NAWET NAJLEPSZYM PRZYJACIOM.

#7 Bezpieczeństwo danych poza Internetem

Oprócz ochrony danych w „życiu wirtualnym”, musimy pamiętać o bezpieczeństwie ich w rzeczywistości.

By bezpieczeństwo naszych danych osobowych było pełne, musimy pamiętać m.in. o:
- rozważnej decyzji w sprawie podpisania deklaracji o zgodzie na przetwarzanie danych osobowych;
- nie mówieniu głośno numerów kont, telefonów czy adresów IP komputerów;
- nie okazaniu publicznie swoich dowodów tożsamości bez wyraźnej potrzeby/argumentu;
- niebraniu udziału w konkursach/loteriach organizowanych przez mało znane firmy (zawsze pojawia się tam obowiązek podania danych osobowych);
- KONTROLI TEGO, CO UDOSTĘPNIŁA SIĘ INNYM.

#8 Dlaczego ochrona danych osobowych jest ważna?

Najkrócej, bez żadnych słownikowych definicji, problem ten przedstawiać można używając:
NASZE DANE OSOBOWE – MY
KRADZIEŻ ICH – KRADZIEŻ NAS
KRADZIEŻ NAS – ZNISZCZENIE NASZYCH PRAW
ZNISZCZENIE NASZYCH PRAW – ZNISZCZENIE ŻYCIA

Praca wykonana na Ogólnopolski Konkurs dla uczniów na infografikę na temat ochrony prywatności i danych osobowych objęty patronatem Generalnego Inspektora Ochrony Danych Osobowych